IRA
Intrusion - Réaction - Appâts

Louis Derathe
THALES Communications
Strategy & Advanced Systems
System & Architecture
160, Blvd de Valmy, BP 82
92704 Colombes

Louis.derathe@fr.thalesgroup.com

RÉSUMÉ

La problématique classique de la protection en bordure des systèmes d'information interconnectés évolue aujourd'hui vers la mise en œuvre du principe de « défense en profondeur » ; la protection des systèmes d'information repose alors sur une succession de couches de protection, renforcées par des outils de veille, d'alarme et de réaction.

Dans une vision intégrée d'un système d'information, la protection de bordure doit ainsi être soutenue par des dispositifs intervenant aussi en interne au SI : systèmes de contrôle comme les IDS[1], système d'alarme et de réaction automatique, systèmes de dérivation des attaques.

De nombreux outils sont disponibles sur le marché ou le Web, mais le problème essentiel reste la mise en cohérence de ces dispositifs.

[1] Intrusion Detection system

Communication présentée lors du symposium RTO IST sur "La défense adaptative pour les réseaux non classifiés", organisé à Toulouse, France, du 19 au 20 avril 2004, et publié dansRTO-MP-IST-041.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 NOV 2004	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
IRA Intrusion - Réaction - Appâts	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **THALES Communications Strategy & Advanced Systems System & Architecture 160, Blvd de Valmy, BP 82 92704 Colombes**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM001845, Adaptive Defence in Unclassified Networks (La defense adaptative pour les reseaux non classifies)., The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**62**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Plan

Liste des Figures

Glossaire

Alerte	Suite à une alarme, avertissement pouvant être de diverses formes : e-mail, trappe SNMP, bip sonore…
Analyse Forensic ou analyse post-mortem	Branche complète de l'informatique, chargée de la récupération des données sur des supports corrompus ou effacé.
Attaque par buffer overflow (ou Débordement de Tampon)	Des vulnérabilités par débordement de tampon apparaissent quand les développeurs utilisent de mauvaises méthodes de codage pour effectuer une fonction dans un programme. Certaines fonctions, notamment en C, ne contrôlent pas la taille de leurs arguments. Ceci crée une faille que certains attaquants sont capables d'exploiter afin d'obtenir un accès sur le système.
Attaque par Déni de Service (DoS pour Denial of Service)	Attaque visant la disponibilité d'un système (réseau, services…).
Cheval de Troie	Programme qui se cache dans d'autres logiciels et qui permet de pénétrer les systèmes informatiques.
Classification	Système de codification indiquant le degré de confidentialité.
Cracker	Personne qui casse les codes d'accès ou les clefs de sécurité des logiciels.
Cryptogramme	Texte chiffré.
Cryptographie	Relatif aux moyens de chiffrement qui permettent de rendre illisible une information à toute personne ne partageant pas le secret pour la déchiffrer.
Cryptographie Asymétrique	Chaque entité possède deux clés : une clé publique de chiffrement qui permet de chiffrer les messages qui lui sont destinés, et une clé privée qui lui permet, à elle seule, de lire les message qui ont été chiffrés avec sa clé publique.
Cryptographie Symétrique	Chaque entité possède la même clé qui permet de chiffrer et de dé chiffrer une information.
Cypherpunk	Hacker qui s'intéresse au cryptage des données informatiques (fichiers, mots de passe, etc).
Evènement	Action sur un système d'information pouvant faire l'objet d'un enregistrement.
Faille	Brèche dans la sécurité d'un système informatique laissée par les concepteurs et la maintenance technique.
Faux-négatif (false negative)	Action malicieuse non détectée par le système de détection d'intrusion.
Faux-positif (false positive)	Action non malicieuse détectée comme étant dangereuse par le système de détection d'intrusion.
FIC, *File integrity checker*, vérificateur d'intégrité de fichier	Outil permettant la surveillance d'un système vis-à-vis de toute modification de ses fichiers. Il surveille l'état de ceux-ci et peut parfois restaurer l'état initial par récupération sur une copie protégée.
Firewall (pare-feu)	« Dispositif informatique qui filtre les flux d'information entre un réseau interne à un organisme et un réseau externe en vue de neutraliser les tentatives de pénétration en provenance de l'extérieur et de maîtriser les accès vers l'intérieur » (*Journal Officiel de la République française*, 16 mars 1999, « Vocabulaire de l'informatique et de l'internet »).Voir garde barrière.
Garde Barrière	Dispositif logiciel ou matériel effectuant un filtrage statique ou dynamique sur les données transitant entre deux réseaux ou plus.
Habilitation de personnel	Reconnaissance de la capacité d'une personne à accomplir en sécurité les tâches fixées
Hacker	Voir pirate informatique.
Homologation	Autorisation d'utiliser, dans un but précisé ou dans des conditions prévues, un produit, un processus ou un service.
HoneyNet	Ensemble d'éléments réels, à but non productif, hautement surveillé et mis en place pour leurrer et observer les agissements d'attaquants.

HoneyPot de production	Honeypot dont le but est d'abaisser les risques pour une société en étant adjoint au système de production.
Honeypot de recherche	Honeypot élaboré dans le but d'acquérir de l'information sur la communauté des attaquants.
HoneyPot ou « pot de miel »	Sens large : ressource dont le but est d'être testée, attaquée ou compromise ; Sens restreint : système connecté à un réseau de production dont le but est de leurrer un attaquant ; Dans le cadre d'un honeynet : machine réelle au sein d'un honeynet
IDS, *Intrusion Detection System*, système de détection d'intrusion	Système qui a pour objectif de déceler une tentative d'intrusion sur l'équipement ou le système à protéger.
Intrusion	Toute utilisation d'un système informatique à des fins autres que celles prévues, généralement dues à l'obtention de privilèges de façon illégitime.
Leurre Informatique	Technique utilisée par les experts pour confondre un pirate. Cela consiste à placer sur un système des fichiers comportant de fausses données qui captiveront l'attention du hacker et qui le maintiendront plus longtemps connecté jusqu'à ce qu'il soit repéré
Backdoor	Voir faille.
Pirate Informatique	Expert en informatique et programmation dont le passe temps est d'explorer les limites des systèmes et des réseaux
Signature d'attaque	Motif d'une attaque (utilisées par les N-IDS).
Sniffing (Ecoute)	Récupération illicite d'informations circulant sur un réseau.
Spoofing	Voir mascarade.
WAREZ	Site qui collecte de nombreuses informations destinées aux hackers.

Chapitre 1 - Introduction

THALES Communication réalise de nombreux systèmes et équipements dans le domaine de la Défense et dispose d'un réel savoir-faire dans les domaines SSI et VAR[2], aussi bien sur les aspects organisationnels que techniques.

THALES Communication est, pour cette raison, à même de proposer dans le cadre de ce symposium une participation sur les sujets technologiques suivants :

- La détection d'intrus, le contrôle et les technologies de réaction
- Les technologies «d'appât» (ressources informatiques conçues pour attirer les pirates et servir d'alarme)

Dans le cadre de la détection d'intrus, THALES Communication présente au chapitre « Tests d'Intrusions dans les Réseaux Informatiques » et au chapitre « Intrusion et Génération de rapports d'Audits » les aspects suivants :

- Inventaire et descriptif des techniques les plus courantes des pirates informatiques dans les domaines des intrusions (interception, balayage, écoute, piégeage, ingénierie sociale, fouille, utilisation et mise en place de canaux cachés, déguisement, mystification, rejeu, déni de service, virus et chevaux de Troie, etc.)
- Inventaire des différents outils (network based IDS, host based IDS, file integrity checkers, analyseurs de logs) et classement selon principes de détection, comportement après détection, sources et fonctionnement (temps réel ou analyse périodique).

Dans le cadre des technologies « d'appât », THALES Communication présente au chapitre « Appâts (honeyPot & Honeynet) » les aspects suivants :

- Définition du concept général de Honey-Pot / Honey-Net, apports de ces technologies et objectifs (protection, étude des profils d'attaques, désinformations)
- Description des aspects d'intégration de ces technologies dans le cadre d'un système d'information (Organisation et personnel, aspects juridiques (notion de piège et responsabilités), problèmes liés aux rebonds et à la remontée d'anonymat, détermination du contenu de ces « appâts », aspects SSI de ces environnements, liens avec systèmes VAR)
- Description des relations entre les technologies IDS et « appât »
- Description des différentes mises en œuvre (Émulation par scripts, Émulation de services et d'environnements, Création d'environnements)

Dans le cadre des protections en bordure, THALES Communication présente au chapitre « passerelle inter-réseaux de sensibilités différentes » et au chapitre « Dissimulation et fuite d'information (Canaux Cachés) » les aspects suivants :

- Concepts techniques et organisationnels des passerelles inter-niveaux
- Architecture de référence d'une passerelle
- Principales techniques de dissimulation d'information

[2] Veille Alerte Réponse

Nota : Les quelques éléments présentés dans ce document ne couvrent pas de façon exhaustive tous les aspects étudiés ou pris en compte, mais devraient permettre aux spécialistes d'appréhender le périmètre de l'étude.

Chapitre 2 - Tests d'Intrusions dans les Réseaux Informatiques

2.1 Généralités

Le projet « Tests d'Intrusions dans les Réseaux Informatiques (TIRI) [1] », réalisé durant le premier semestre 2000, avait pour buts, d'une part de réaliser un état de l'art sur les différentes techniques d'attaques des systèmes d'information, et d'autre part de définir et de mettre en œuvre une plate-forme de tests d'intrusions et de sensibilisation.

Les techniques présentées ont été regroupées en deux catégories : les attaques physiques et les attaques logiques. On parle d'attaque physique dès lors que l'attaque concerne le médium de communication du système d'information. Il peut par exemple s'agir d'interceptions, de brouillages, de balayages ou d'écoutes. Les attaques logiques consistent le plus souvent à exploiter des défauts de configuration ou de conception dans les réseaux ou dans les logiciels. Les types d'attaques logiques les plus connus sont les fouilles de données, les canaux cachés, les usurpations d'identités, les rejeux de séquences, les chevaux de Troie, les dénis de service, les fuites d'informations, les virus, les vers et la cryptanalyse.

Le projet s'est particulièrement attaché à la méthodologie utilisée par les attaquants pour s'introduire frauduleusement dans les systèmes d'information. Dans la grande majorité des cas, il est possible de distinguer quatre phases distinctes dans une intrusion. La première est une phase de recherche d'anonymat qui consiste pour l'attaquant à s'assurer que l'attaque qu'il compte mener lui procurera un très haut degré d'anonymat. La deuxième phase est une phase de recherche d'informations qui consiste le plus souvent à réaliser une cartographie complète des services du réseau ou de la machine cible. Cette étape permet à l'attaquant de sélectionner l'attaque la plus adaptée qu'il pourra alors lancer lors de la phase d'infiltration. Enfin une attaque se termine souvent par une phase d'effacement des traces qu'elle a laissées.

L'intérêt d'étudier les méthodologies d'intrusions est de définir les moyens de protection conséquents. Les techniques de protection sont aussi variées que les techniques d'attaques. Tout comme il existe des grands principes pour les attaques, il existe également des grands principes pour les protections : principe du moindre privilège, principe de la défense en profondeur, principe du maillon faible… De la même façon, tout comme il existe des outils pour automatiser les attaques, il existe des outils pour automatiser les protections : pare-feu, outils de chiffrement, scanners… Les procédures et les outils à mettre en oeuvre pour sécuriser un site doivent être clairement définies dans un document appelé « politique de sécurité ».

2.2 Quelques Eléments constitutifs de l'étude

Les pirates informatiques utilisent différentes techniques pour obtenir la cartographie d'un réseau. Selon les outils utilisés, les traces seront plus ou moins visibles dans les fichiers de journalisation ; aussi, l'attaquant va-t-il essayer le plus souvent de passer tout simplement par l'entrée principale et si possible de façon normale (il essaiera d'obtenir un mot de passe), sinon, il utilisera les failles ou trappes de certains logiciels.

2.2.1 Quelques Exemples d'Attaques Physiques

Interception L'attaquant cherche à intercepter un signal électromagnétique et à l'interpréter. L'interception peut porter sur des signaux hyperfréquences, ou hertziens, émis, rayonnés, ou conduits. L'agresseur se mettra ainsi à la recherche des émissions satellites, et radio, mais aussi des signaux parasites émis par les SI, principalement par les terminaux, les câbles et les éléments conducteurs entourant les SI.

Brouillage Utilisée en télécommunication, cette technique rend le SI inopérant. C'est une attaque de haut niveau, car elle nécessite des moyens importants, qui se détectent facilement.

Balayage « scanning »Le balayage consiste à envoyer au SI un ensemble d'informations de natures diverses afin de déterminer celles qui suscitent une réponse positive. L'attaquant pourra aisément automatiser cette tâche, et déduire, par exemple, les numéros téléphoniques qui permettent d'accéder à un système, le type du système, et pourquoi pas, le nom de certains utilisateurs ainsi que leur mot de passe.

Écoute « sniffing » L'écoute consiste à se placer sur un réseau informatique ou de télécommunication et à analyser et à sauvegarder les informations qui transitent. De nombreux appareils du commerce, généralement conçus pour l'administration réseau, facilitent les analyses et permettent notamment d'interpréter en temps réel les trames qui circulent sur un réseau informatique.

Piégeage L'agresseur tentera d'introduire des fonctions cachées dans le SI, en principe en phase de conception, de fabrication, de transport ou de maintenance.

2.2.2 Quelques Exemples d'Attaques Logiques

Ingénierie sociale L'ingénierie sociale consiste à obtenir des informations sur un système d'information en exploitant les faiblesses des utilisateurs. On peut, par exemple, envoyer un mél dont l'expéditeur est supposé être l'administrateur et demander au destinataire de changer son mot de passe, voire de lui en communiquer un nouveau pour la maintenance du réseau.

Fouille La fouille informatique, par analogie avec la fouille physique, consiste à étudier méthodiquement l'ensemble des fichiers et des variables d'un SI pour en retirer des données de valeur. Cette recherche systématique d'informations est en général grandement facilitée par la mauvaise gestion des protections classiques qu'il est possible d'attribuer à un fichier.

Craquage de mots de passe Une fois le mot de passe crypté récupéré, il est nécessaire de le retrouver sous sa forme originale. Deux approches d'attaques sont envisageables. La première consiste à s'appuyer d'un dictionnaire, à crypter systématiquement ses éléments et à vérifier si le résultat coïncide avec le mot de passe capturé. La seconde méthode, appelée méthode par force brute, essaye toutes les combinaisons possibles de caractères jusqu'à obtenir le bon résultat.

Déguisement Il s'agit d'une attaque informatique qui consiste à se faire passer pour quelqu'un d'autre, et obtenir les privilèges de celui ou celle dont on usurpe l'identité.

Mystification L'attaquant va simuler le comportement d'une machine pour tromper un utilisateur légitime et s'emparer de son identifiant et de son mot de passe.

Rejeu Le rejeu est une variante du déguisement qui permet à un attaquant de pénétrer dans un SI en envoyant une séquence de connexion effectuée par un utilisateur légitime et préalablement enregistrée à son insu.

Substitution Ce type d'attaque est réalisable sur un réseau ou sur un système d'information comportant des terminaux distants. L'agresseur écoute une ligne et intercepte la demande de déconnexion d'un utilisateur travaillant sur une machine distante. Il peut alors se substituer à ce dernier et continuer une session normale sans que le système note un changement d'utilisateur.

Saturation : déni de service (Dos ou Ddos) Cette attaque contre la disponibilité consiste à remplir une zone de stockage ou un canal de communication jusqu'à ce qu'on ne puisse plus l'utiliser.

Cheval de Troie Un cheval de Troie est un programme qui se cache dans un autre programme, apparemment inoffensif, qui, dès que ce dernier est lancé, s'exécute de façon clandestine.

Trappe & faille Une trappe est un point d'entrée dans un système informatique auquel les mesures de sécurité normales ne sont pas appliquées. Une trappe peut être par exemple, délibérément mis en place par les programmeurs ou les personnes chargées de la maintenance, pour des raisons de simplicité et de rapidité d'action (réalisation de tests par exemple), et qu'ils ont oublié de supprimer.

Bombe Une bombe est un programme destructif en attente d'un événement spécifique déterminé par le programmeur pour se déclencher.

Virus Un virus est un programme parasitant les machines et capable de se reproduire. Il est en mesure d'infecter d'autres programmes, qui à leur tour se conduiront comme le virus père, et peuvent endommager les systèmes.

Ver Un ver est un programme capable de se propager de réseau en réseau et de les rendre indisponibles.

Asynchronisme Ce type d'attaque évoluée exploite le fonctionnement asynchrone de certaines parties ou commandes du système d'exploitation. Les requêtes concernant de nombreux périphériques sont mises en file d'attente dans l'ordre des priorités puis traitées séquentiellement. Des tâches sont ainsi endormies puis réveillées lorsque les précédentes requêtes sont satisfaites. A chaque fois qu'une tâche ou qu'un programme est ainsi endormi, son contexte d'exécution est sauvegardé pour être restitué en l'état lors du réveil. Ces sauvegardes de contexte contiennent donc des informations propres à l'état du système et un attaquant averti peut les modifier afin de contourner les mesures de sécurité.

Cryptanalyse La cryptanalyse est une discipline de la cryptographie dont le but est de retrouver le message clair à partir du message chiffré sans détenir tous les éléments (clés, algorithme).

2.3 Environnement Technique étudié

Selon des scénarios mettant en œuvre le déroulement classique d'une attaque (Anonymat / Recherche d'informations / Infiltration / Effacement des traces), la plate-forme de démonstration a permis de montrer les mode d'actions d'outils comme ceux présentés ci-dessous.

Bombes emails

- ***Kaboom*** programme pour bombarder une boîte aux lettres
- ***Anonymail*** permet de créer des méls sous une fausse identité
- ***Homicide*** utilitaire qui permet de bombarder une personne en dissimulant l'adresse source des messages
- ***Avalanche*** utilitaire qui permet de bombarder un compte de messagerie, et permet également d'inscrire le compte cible à différentes listes de diffusion

Craquage de mots de passe

- ***NTUCrack*** utilitaire qui permet de craquer les mots de passe Unix
- ***John The Ripper*** un des programmes les plus célèbres pour craquer les mots de passe de type Unix.
- ***L0phtCrack*** l'utilitaire le plus célèbre pour craquer, entre autres, les mots de passe de Windows NT

Déni de service

- ***Winnuke*** provoque l'arrêt de Windows 95 et de Windows NT 3.51 et Windows NT4 (si le service Pack est inférieur à 4 car Microsoft a depuis corrigé la faille exploitée)
- ***Killwin*** pour Linux paralyse en quelques secondes une machine NT 4.0 pack 6 en envoyant des messages de dépassement de bande (MSG_OOB)
- ***Bitchslap*** utilitaire réalisé par des hackers des groupes SIN et technophoria permet d'envoyer un message de dépassement de bande (MSG_OOB) vers le port 139 d'un poste Windows
- ***Portfuck***

Sniffeurs

- ***Ethereal*** fonctionne aussi bien sous Windows que sous Linux
- ***Analyser***

Scanners

- ***Ultrascan*** logiciel de balayage de ports. Il peut scanner une plage d'adresses IP et une plage de ports
- ***Nmap*** logiciel de balayage est assez sophistiqué car il peut, par exemple, effectuer des balayages par demi-connexions

Chevaux de Troie

- Netbus

Chapitre 3 - Intrusion et Génération de Rapports d'Audit

3.1 Généralités

Le projet « Tests d'Intrusion et Génération de Rapports d'Audit (TIGRA) [4] » réalisé durant le premier semestre 2002 s'est intéressé aux systèmes de détection d'intrusions communément dénommés « IDS ». La première phase du projet a consisté à réaliser un état de l'art sur les IDS. L'objet de la deuxième phase fut de mettre en œuvre un IDS au sein d'une plate-forme de tests afin d'en présenter les différents aspects.

Les trois fonctionnalités principales des IDS sont la détection des attaques, la réaction aux attaques et l'analyse des attaques. Certains IDS sont capables de réagir aux attaques en les bloquant (d'un point de vue fonctionnel, ces IDS qui fonctionnent en mode coupure, se rapprochent des pare-feux) mais dans la majorité des cas, un IDS est capable de journaliser les tentatives d'attaques, d'évaluer leur niveau de gravité et de déclencher des alertes appropriées.

La détection des attaques consiste le plus souvent à détecter les signatures des attaques mais des méthodes d'analyse comportementale commencent à apparaître (C-IDS). La réaction aux attaques peut se faire soit de manière active (blocage de l'attaque ou dérivation) soit de manière passive (journalisation et génération d'alertes uniquement). Les sources de données des IDS sont variées : il peut s'agir d'audits systèmes (systèmes de fichiers), d'audits applicatifs (contrôle des débordements de mémoire) ou encore des flux de données transitant sur le réseau.

Les deux types d'IDS les plus couramment rencontrés sont les « Network Based IDS » (N-IDS) et les « Host Based IDS » (H-IDS). Les premiers sont installés au niveau des goulets d'étranglement (bordures) des réseaux pour analyser les flux entrant et sortant, tandis que les seconds sont positionnés sur les hôtes, et sont chargés d'analyser des sources de données plus variées (systèmes de fichiers, mémoire vive, processus …).

Les IDS présentent quelques limites. Lorsqu'ils sont mal paramétrés, ils peuvent générer des quantités importantes de « faux-négatif » et de « faux-positifs ». Enfin, d'un point de vue pratique, les IDS peinent à analyser des débits importants, et peuvent occasionner des pertes de qualité de service. De plus, il est possible pour un attaquant de générer un grand nombre d'attaques dont il sait qu'elles sont très coûteuses en ressources pour l'IDS, et ainsi provoquer une rupture de service de l'IDS.

3.2 Quelques Eléments constitutifs de l'étude

3.2.1 Fonctions utiles des IDS en matière de SSI

1 / Détection des attaques :

- ***détection*** précoce de l'attaque afin de limiter sa propagation à un nombre restreint d'hôtes
- ***journalisation*** des actions entreprises par l'attaquant
  - afin d'analyser les moyens mis en oeuvre et comprendre la méthode employée pour adapter la protection actuelle
  - avec gradation des enregistrements selon le niveau de gravité

2 / Réaction aux attaques :

- ***clôture de la connexion*** (Session Snipping)
- ***reconfiguration dynamique des règles du pare-feu***

- ***ou autre selon*** des ***scénarios d'attaques***

3 / Avertissement local et / ou distant vers le Responsable SSI

4 / Analyse

3.2.2 Modes d'action des IDS

Trois modes d'actions sont caractéristiques des outils de détection d'intrusion :

- ***mode furtif*** correspond à un mode où l'IDS n'offre aucune interaction directe avec le système (ainsi un paquet qui le traverse conserve son adresse MAC)
- ***mode coupure*** : toutes les trames sont contrôlées avant de pouvoir passer (comme dans le cas d'un pare-feu)
- ***mode écoute***, sur un brin du réseau où il est possible d'enregistrer tout ou partie du trafic, il collecte toute l'information transitant sur le brin (il n'agit pas en mode coupure : fonction d'alerte en cas d'attaque, mais pas de rejet de la trame « suspecte »).

3.2.3 Classement des IDS

Il s'effectue selon :

- ***le principe de détection*** comportementale (C-IDS) et par scénarios (essentiellement basé sur signature)
- ***le comportement après détection*** suivant s'il est actif (réaction de riposte à l'attaque) ou passif (journalisation uniquement)
- ***les sources de données*** pouvant provenir soit d'un audit système (exemple : modification du système de fichiers…), soit applicatif (contrôle des débordement de mémoire) ou encore de paquets transitant sur le réseau (N-IDS)
- ***la fréquence d'utilisation*** selon si elle s'effectue en temps réel ou par analyse périodique

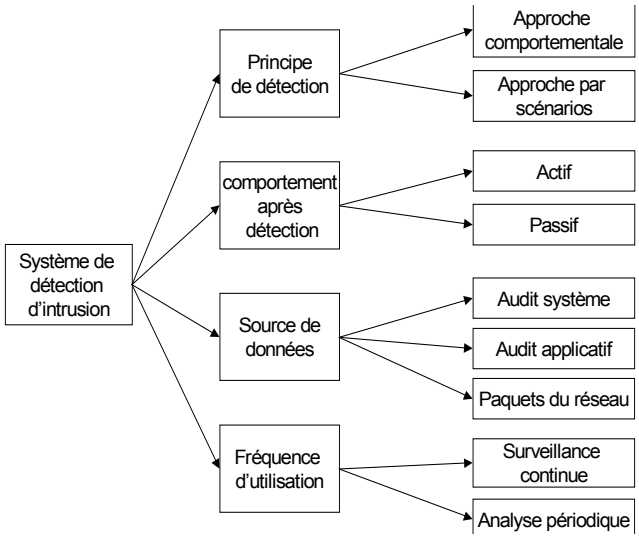


Figure 1 : principes de fonctionnement des systèmes de détection d'intrusion

3.2.4 Les différents types d'IDS

Les N-IDS (Network Based IDS):

- ils détectent les actions malicieuses au niveau du réseau (capture des trames et comparaison à une base d'actions intrusives appelées *signatures d'attaque)*
- Les signatures se basent parfois sur la norme CVE (*Common Vulnerability Exposure*) qui décrit des attaques connues
- Contrairement aux H-IDS, ils ne gèrent pas les attaques opérées sur un terminal (modifications fichiers…)
- Ex : ***Snort, BlackIce, Cisco Secure IDS ou NetRanger, Shadow, RealSecure***

Les H-IDS (Host Based IDS):

- Ils surveillent l'état d'un hôte :
  - contrôle de la gestion de la mémoire (afin d'éviter des dépassements de mémoire : *buffer overflow*)
  - contrôle de la journalisation
  - contrôle des droits des utilisateurs
- Ex : ***Swatch, RealSecure OS Sensor, Intruder Alert***

Les File Integrity Checkers:

- Ils utilisent des outils cryptographiques afin d'établir une base de signatures des données à protéger (*motifs de scellement*). Ceci leur permet de déceler des modifications non autorisées de la table de fichiers
- Ex : ***Tripwire, AIDE, Intact*** ou ***Integrit***

Les autres types d'IDS :

- **Honeypots** (logiciel *Deception Toolkit*) et les **Honeynets** émulent des services dans le but de leurrer un attaquant et de le retarder
- Les **Hybrid IDS (***CyberCop Monitor ou CentraxICE***)** qui regroupent les fonctionnalités d'un N-IDS et d'un H-IDS sur un seul hôte. Très utiles dans le cas d'une architecture commutée où un N-IDS traditionnel ne peut opérer
- Les **Network Node IDS** (NN-IDS) chargé de la supervision d'un groupe de machines
- les **C-IDS** (pour *Comportemental IDS*). Ils surveillent et tentent d'analyser le comportement des utilisateurs internes et externes au réseau :
  - **Détection par anomalie** : elle se base sur l'adage « *tout ce qui n'est pas normal est dangereux* ». Cette démarche, conduit, par exemple, à journaliser tous les accès aux « services exotiques » (i.e. ports non associés à un service connu par exemple)
  - **Détection par mauvaise utilisation** : « *tout ce qui n'est pas dangereux est normal* »
- ***Spade*** (pour *Statistical Packet Anomaly Detection Engine*), ce module effectue un recensement statistique des données sur le réseau local et établit ainsi ce qui correspond à un « fonctionnement normal » ; schématiquement, toutes les données rares sont suspectes.

3.3 Environnement Technique étudié

Une plate-forme de test a permis d'apprécier les fonctionnalités types d'un IDS : ***Snort***[3] compilé avec les options de réponses actives (module « flexresp » permettant la clôture de « sessions malicieuses ») et d'envoi de trappes SNMP en cas d'alerte.

3.3.1 Les attaques mises en oeuvre :

Détection des balayages de ports (« scan de ports »)

- ***Balayage de connexion TCP*** : simulation d'une demande de connexion
- ***Balayage TCP/SYN*** méthode consistant à envoyer un paquet marqué du drapeau SYN sur les ports de l'hôte à sonder. Si le système renvoie un SYN/ACK pour un service donné c'est que le port est à l'écoute
- ***Balayage TCP/FIN*** : balayage basé sur le type de réponse renvoyée en cas d'envoi d'un drapeau FIN à 1
- ***Balayage Xmas Tree*** : envoi à la cible d'une trame avec une suite de zéros ainsi que les drapeaux Urgent (URG), Push (PSH), et FIN à 1
- ***Balayage NULL*** : la trame a tous ces drapeaux à 0 et une séquence de 0

Attaque par validation d'entrée *Unicode* : *Unicode* a pour objectif de former un jeu de caractères unique pour tous les langages existants. L'origine de la faille se trouve dans les logiciels associés à Unicode comme le serveur Web Microsoft IIS

Vulnérabilité test-cgi Cette vulnérabilité permet de recenser l'ensemble des fichiers du serveur attaqué

Vulnérabilité du script *codebrws.asp* permet d'éditer n'importe quel fichier contenu sur le poste de la victime

Remontée de répertoires

Attaque par débordement de tampon (attaque iishack sur le serveur Web Microsoft IIS 4.0) un utilisateur tente de placer plus de données dans un tampon que ce qu'il ne peut en recevoir

Remontée d'informations vers l'attaquant correspond en général à des flux non autorisés par la politique de sécurité de l'entreprise

3.3.2 Mise en évidence des limites de fonctionnement des IDS actuels

quatre limites ont été testées au niveau de la plate-forme :

Augmentation de la fenêtre de temps, test est effectué avec ***nmap***, avec options « Paranoid » (balayage port toutes les 5 minutes) et « Polite » (balayage port toutes les 15 secondes)

Modification de la signature de l'attaque

Attaque DoS, tests effectués avec un « stresseur d'IDS » (***Stick***) :

- ***attaque portant sur le niveau IP*** : falsification de l'adresse IP (l'adresse IP source est égale à l'adresse IP de destination)

[3] www.snort.org

- ***attaque portant sur le niveau TCP*** : tentative de connexion sur un service fermé, ici telnet (port 23 TCP)
- ***attaque portant sur les niveaux supérieurs*** : attaque lancée sur une trame HTTP

Attaque répartie, attaque réalisée par plusieurs assaillants

Chapitre 4 - Appâts (HoneyPot & Honeynet)

4.1 Généralités

Le projet « HoneyPot & Honeynet (HP&HN) [3] » réalisé durant le premier semestre 2002 s'est intéressé aux principe du « pot de miel » : mise en œuvre de dispositifs destinés à leurrer les attaquants pour les écarter des cibles sensibles et pour mieux étudier leurs comportements. L'objectif du projet était d'une part de réaliser un état de l'art sur les HoneyPot & Honeynet et d'autre part de réaliser une plate-forme de démonstration.

Les HoneyPot & Honeynet ont l'avantage de générer des données de connexions pertinentes avec en général un bruit faible. Contrairement aux systèmes de détection d'intrusions, ils ne sont pas submergés par des flux réseaux et offrent donc en général une bonne disponibilité. Les deux principaux inconvénients liés aux HoneyPot & Honeynet sont d'une part la perte de ressources matérielles et d'autre part, s'ils sont mal maîtrisés, la possibilité pour un attaquant de se servir de ces dispositifs comme un rebond pour mener ses attaques vers d'autres systèmes.

Parmi les HoneyPot & Honeynet on peut distinguer ceux de production et ceux de recherche. Les HoneyPot & Honeynet de production sont destinés à leurrer les attaquants pour les écarter des zones sensibles du site en leur proposant des défis plus simples. On parle alors souvent de «honeypots ». Les pots de miels de recherche sont destinés à étudier le comportement des attaquants pour mieux comprendre leurs méthodes et leurs stratégies. Les « honeynets » par exemple recréent aux mieux les conditions d'un réseau d'entreprise en mettant souvent plusieurs machines et matériels réseau à la disposition de l'attaquant.

L'aspect le plus délicat des HoneyPot & Honeynet est sans doute le paramétrage de leur niveau de sécurité. En deçà du seuil dit de la « limite d'écoute », les informations qu'ils génèrent sont polluées par les attaques à faible niveau de compétences qui sont parfaitement connues des responsables systèmes et qui n'apportent aucune information supplémentaire sur le comportement des attaquants. Au-delà du seuil dit de la « limite de risque acceptée », le HoneyPot & Honeynet devient fortement compromis et peut mettre en danger le reste du système d'information (Cf. plus loin les aspects « gradation de la difficulté d'accès).

D'un point de vue pratique les honeypots sont souvent basés sur des scripts qui émulent des services et des environnements ainsi que sur des environnements dits de « prison ». Les architectures des honeynets sont plus variées et complexes et mettent en œuvre des mécanismes de contrôle de données et de capture d'informations. Les mécanismes de contrôle de données ont pour but de maîtriser les flux des attaquants pour les empêcher d'attaquer d'autres systèmes. Les mécanismes de capture d'informations servent à archiver de façon sûre les actions menées par les attaquants pour ensuite pouvoir procéder à une analyse de leurs comportements.

4.2 Quelques Eléments constitutifs de l'étude

4.2.1 Périmètre réel des HoneyPots et HoneyNets

Le concept de HoneyPot et HoneyNet dépasse largement celui des outils censés les concrétiser, la « cartographie »[4] présentée ci-dessous propose un périmètre plus juste des aspects à prendre en compte :

[4]. Cette réflexion peut s'inscrire dans le cadre plus global de l'étude d'une « Cartographie de la Maîtrise de l'Information », HoneyPot (et HoneyNet) représentant alors un « composant » mis à disposition.

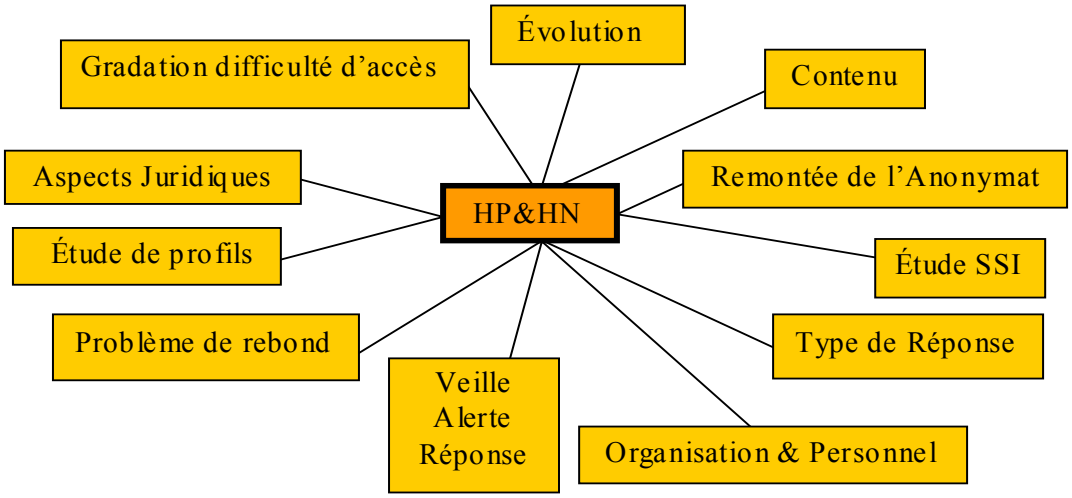


Figure 2 : Les aspects des HoneyPots et HoneyNets.

Organisation et personnel : compétence nécessaires (profils), processus de sélection (conservation du secret)

Aspects juridiques : notion de piège et éléments de preuve, responsabilité de l'organisme

problèmes de rebond : risques judiciaires, information des sites concernés (amont, aval)

Remontée de l'anonymat : droits et outils adaptés

Contenu : composition de la partie réelle et de la partie désinformation

Gradation de la difficulté d'accès : modulation du niveau de sécurité de l'HoneyNet (étape **(1)**), pour sélection d'une catégorie d'attaquants particulière (étape **(2)**)

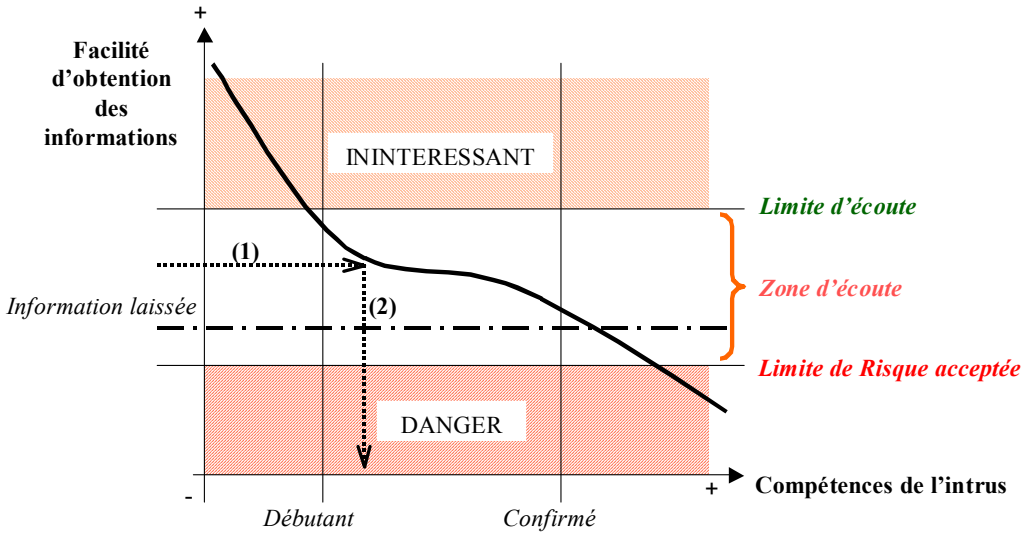


Figure 3 : Sécurisation de l'information et compétences de l'intrus.

Évolution : en fonction des « modes », de l'étude des attaques et de l'évolution des stratégies d'attaque

Étude de la Sécurité des Systèmes d'Information (SSI) : test de moyens de protection ou copie conforme de la politique SSI interne

Type de réponse : coupure de connexion, envoi d'un message d'avertissement, riposte

Veille, Alerte, Réponse (V.A.R.) : liens avec système VAR de l'organisme

Étude du profil : analyse du profil des attaquants, liens avec systèmes de protection

4.2.2 Le HoneyPot

Le honeypot est, à l'heure actuelle, un produit aux fonctionnalités plus ou moins avancées et présentant surtout des degrés d'interaction avec l'attaquant différents.

- **Émulation par scripts** : un ensemble de scripts émule un certain nombre de vulnérabilités connues. (ex version ancienne d'un serveur de messagerie *Simple Mail Transfer Protocol* (SMTP) à même de fournir un fichier de mots de passe comportant de fausses empreintes) ; l'intérêt d'un tel outil réside dans le leurre et dans la déception[5]
- **Émulation de services et d'environnements :** produits, libres ou commerciaux, permettant de recréer un discours logique avec l'attaquant par réplication de la pile IP.
- **Création d'environnements dits « prisons » :** exécute une image, appelée « prison », d'un système d'exploitation au sein d'un autre ; Cette image est surveillée et ne déborde pas vers le système hôte, elle propose un environnement complet à l'attaquant.

4.2.3 Architecture et modèle des HoneyNets

Les HoneyNets constituent des systèmes réels, rien n'est émulé ; leurs architectures reposent sur deux aspects critiques, le contrôle des données, et la capture des informations.

La figure suivante montre ce que pourrait être un honeynet. Trois réseaux séparés par un pare-feu :

- l'Internet, réseau d'où surviennent les attaques
- le honeynet, ensemble de machines dont le but est d'être testé, attaqué ou compromis (HP = honeypots)
- le réseau d'administration, réseau de confiance où seront recueillies les données du honeynet et permettra l'administration de celui-ci.

[5] entendre ici l'acquisition de données sur lesquelles l'attaquant dépensera du temps pour un profit nul

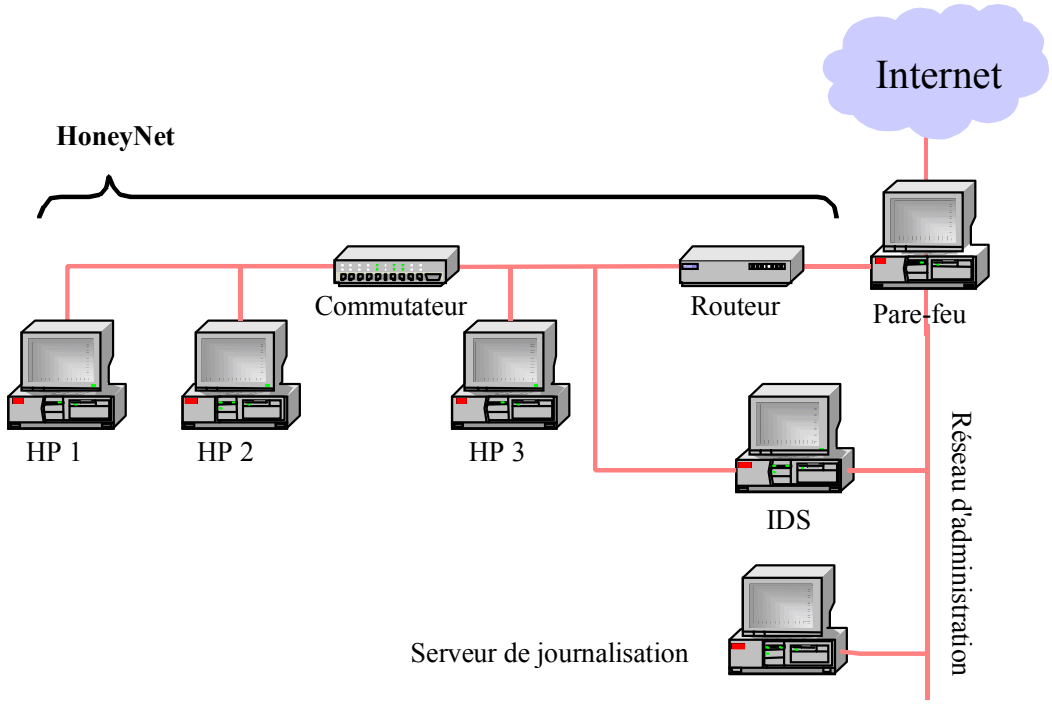


Figure 4 : Architecture d'un HoneyNet.

Contrôle des données en provenance de l'Internet : il ne sera pas utile de tout observer ou laisser passer, il faudra limiter le trafic en provenance de l'Internet

Contrôle des données en provenance des honeypots : éviter les rebonds, permettre la capture de données manipulées

4.3 Environnement Technique étudié

honeypots.

- ***Deception ToolKit*** de Fred COHEN, programme d'émulation par scripts, est un produit libre du monde Linux.
- ***Back Officer Friendly*** de NFR Security, est libre de téléchargement pour un usage personnel, prévient l'administrateur de toute tentative de prise de contrôle de la machine par « *Back Orifice* »[6], donne à l'attaquant de fausses informations, tout en enregistrant les adresses de provenance de l'intrus et ses différentes manipulations.(contient aussi des programmes simulant des services, comme transfert de fichiers (FTP), web (HTTP), ou courrier (SMTP))
- ***Honeyd*** est un démon Linux qui crée des hôtes virtuels, il permet de simuler un réseau complet répondant aux fonctionnalité TCP/IP (réponses PING et TraceRoute par exemple).
- ***Recourse ManTrap*** produit de la catégorie des systèmes de détection d'intrusion, il crée des environnements prisons surveillés pour repérer, contenir et suivre toute attaque. Cet outil permet aussi de gérer les réponses à mettre en œuvre : suivant le degré de l'attaque, il pourra alerter,

[6]. « *Back Orifice* » est un programme répandu. Il permet, par l'installation d'un serveur sur la machine Windows convoitée, de donnée un accès complet à l'attaquant exécutant le client correspondant. Ceci lui permettra de revenir, en utilisant cette porte dérobée, comme bon lui semble.

enregistrer le déroulement de l'attaque, terminer la session, ou exécuter toute autre action personnalisée.

- ***Specter*** émule différents systèmes, des plus répandus, comme Windows 98, NT, 2000, MacOs, Linux et autres UNIX comme Solaris, NeXTStep, Tru64, Irix, AIX.

Pour les honeynets

- Contrôle d'accès : ***CheckPoint FireWall-1*** est un pare-feu très répandu ; en plus des fonctionnalités primaires, il permet un enregistrement dans des journaux, nécessaires pour l'étude post-attaque, le suivi des connexions actives, ou la surveillance de la sécurité des exécutables Java ou ActiveX.
- Couche réseaux : ***IDS SNORT*** système de détection d'intrusion pour réseau (NIDS) ; léger et aisé à mettre en place
- Couche Hors-ligne : ***TripWire,*** outil libre pour le monde Linux, vérifie l'intégrité du système ; ***The coroner's Toolkit*** boîte à outils pour l'analyse post-mortem du système

Chapitre 5 - Passerelle inter-réseaux de sensibilités différentes

5.1 Généralités

La sécurité des échanges entre systèmes d'information est un problème d'actualité d'autant plus critique que l'on assiste de nos jours à une dématérialisation de plus en plus généralisée de l'information et des services associés. Cette dématérialisation s'opère bien évidemment dans des secteurs publics sensibles tels que le secteur bancaire, avec les transactions en ligne ou le secteur de l'assurance maladie, avec la création de la carte électronique de l'assuré, mais le secteur de la Défense ne fait pas exception à la règle puisqu'il connaît une demande croissante en la matière : le cadre opérationnel tactique implique de plus en plus d'échanges et de partage d'informations sensibles (intervention dans le cadre de coalitions).

Malheureusement, la recrudescence et la diversité des attaques (déni de service, compromission…) tendent à fragiliser les réseaux de communication actuels et l'on doit donc recourir à des solutions d'échanges sécurisés de l'information.

Or, à l'heure actuelle, les diverses réglementations ne préconisent pas (loin s'en faut) l'échange directe d'information entre deux systèmes de sensibilité différente, elle impose parfois même une rupture physique afin de prévenir une éventuelle fuite d'information ou se prémunir d'éventuelles attaques externes. Cette rupture physique empêche l'automatisation de l'échange des données, et nuit alors aux performances du service offert par le système.

C'est donc afin de pallier cette limitation que THALES a étudié, dans le cadre du programme « Système d'Echange Sécurisé pour un Accès Multi niveaux Expérimental (SESAME) [5] » la possibilité de créer une passerelle dite « multi niveaux » sécurisée qui réponde aux contraintes fortes liées à l'interconnexion de ce type de systèmes.

Cette passerelle met donc en oeuvre un mécanisme d'échange d'information sécurisé entre des systèmes de sensibilité différente reposant principalement sur une notion de SAS cloisonnant les deux systèmes ; ce SAS devant être automatisé autant que possible afin limiter le besoin d'intervention humaine.

5.2 Quelques Eléments constitutifs de l'étude

5.2.1 Rappel sur la réglementation

Afin de réaliser des systèmes sécurisés et homologués pour une utilisation dans cadre classifié de défense, toutes les exigences de sécurité, d'un point de vue technique et organisationnel, sont traduites au sein de textes de loi (dispositions législatives et réglementaires[7]) ; elles doivent être prises en compte en particulier lors de l'interconnexion de systèmes d'information.

5.2.2 Etat de l'art

Interconnecter physiquement deux réseaux de sensibilité différente est à l'heure actuelle souvent interdit, la seule solution sûre et généralement autorisée pour un échange d'information reste à ce jour la rupture physique entre les deux systèmes (mesure organisationnelle) : la transmission d'information s'effectue alors par support externe (par exemple par disquette ou cédérom) détenu par une personne habilitée (au niveau de sensibilité le plus élevé mis en jeu dans le cadre de cet échange).

[7] *Rappel* : dans le cadre de l'OTAN, les deux textes de référence sont « Security within the North Atlantic Treaty Organisation (NATO) - C-M(2002)49 du 17 juin 2002" pour ce qui concerne l'homologation des SI, et « Directive sur les aspects techniques et la mise en oeuvre de l'INFOSEC pour l'interconnexion des systèmes d'information et de communication (SIC) - AC/322-D/0030-REV1 » pour ce qui concerne les interconnexions.

5.2.3 Concepts techniques et organisationnels

Une architecture d'échange sécurisée devra, donc, mettre en œuvre les éléments constitutifs suivants :

- Un « SAS automatisé » : un système d'échange par lequel transite l'information sans qu'il y ait jamais de lien continu établi entre système émetteur et système récepteur. Le SAS répond donc au besoin de coupure physique et rend le système étanche aux attaques extérieures.
- Un système de marquage ou de « labellisation » : permettant de caractériser la nature de l'information en associant à celle-ci une description formelle plus ou moins détaillée de son contenu et de sa sensibilité.
- Une autorité « Valideur » : autorité en charge de décider si le caractère d'une information donnée autorise une transmission vers le système de sensibilité inférieure
- Un système « Infrastructures à clé publique, ou PKI (Public Key Infrastructure) » : Infrastructure qui permet d'établir une relation de confiance dans le cadre d'une politique de sécurité. Une telle infrastructure est composée de plusieurs éléments :
  - en premier lieu une autorité de certification qui est chargée de générer les certificats, en associant l'identité d'une personne ou d'un système à une signature numérique ;
  - le second élément est l'autorité d'enregistrement qui capture et identifie l'identité des utilisateurs et soumet les demande de certificats à l'autorité de certification ;
  - le troisième composant d'une PKI est le système de distribution des clés.
- Un système de « Pare-feu » : système permettant de protéger un ordinateur des intrusions provenant du réseau.

5.2.4 Une Passerelle de type hybride conséquente

La différence de sensibilité des flux montant et descendant nous mène à différencier le traitement à réaliser pour chaque sens d'échange de données.

Ainsi, on utilisera une architecture de type diode simple au niveau du flux montant (ce flux étant généralement autorisé). Par contre, le sens descendant étant plus sensible, on a recours à une architecture plus contraignante, associant une diode à un SAS. Le principal avantage de cette architecture étant lié à l'apport de notion de coupure physique entre les deux systèmes grâce au sas modélisé par les 3 pare-feux.

Passerelle de type hybride

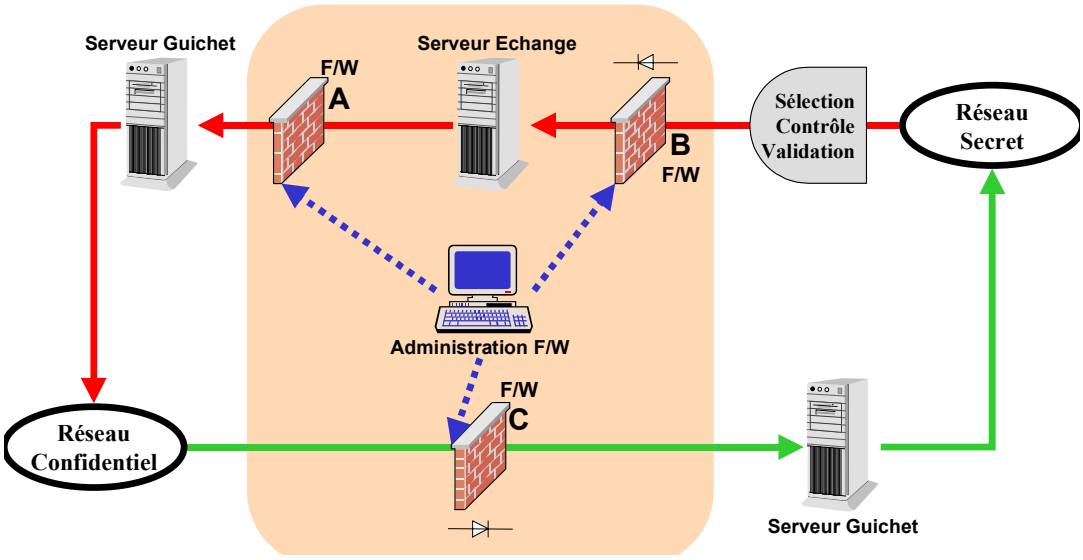


Figure 5 : Passerelle de type hybride

Description :

- Cette modélisation apporte une optimisation des ressources utilisées pour le transfert des informations tout en essayant de conserver la notion de coupure physique. En effet, les deux pare-feu ne sont jamais passants en même temps et sont ouverts et fermés en alternance. Ainsi on garantit bien que l'on a jamais un lien constant entre les deux systèmes d'information
- La passerelle, pour les échanges dans le sens descendant, s'apparente à une DMZ classique. En effet, le serveur d'échange sert de proxy et est protégé par un pare-feu A. Le pare-feu B supplémentaire fonctionne en mode « diode » et permet d'assurer un échange unidirectionnel (et protège le réseau haut des attaques).

5.3 Environnement Technique étudié

protocole de transfert	***FTP*** (File Transfert Protocol)
développements	***Java*** sur plate-forme LINUX (avec le logiciel I.D.E. ***Jbuilder*** pour la réalisation de l'IHM)
structuration des messages échangés	***XML***
protection par pare-feu*x*	***iptables*** de LINUX avec règles de filtrage réalisées grâce au logiciel ***Firewall Builder***

Chapitre 6 - Dissimulation et fuite d'information (Canaux Cachés)

6.1 Généralités

« L'étude sur la dissimulation et la fuite d'information par l'intermédiaire de canaux cachés (EFFICACE) [6] » avait pour objet la réalisation d'un état de l'art sur ces notions. Un panel des techniques permettant ces actions, comme la stéganographie et l'encapsulation protocolaire, ont été ainsi étduiées, des solutions préventives ont été préconisées et mises en application afin de limiter le champ d'action d'un éventuel attaquant et par conséquent la violation de la politique de sécurité mise en oeuvre.

Ce projet s'inscrit dans la continuité logique des études présentées plus haut. Elle a été menée sur la plate-forme Tests d'Intrusions dans les Réseaux Informatiques (TIRI) et fait suite aux études sur l'intrusion et Génération de Rapports d'Audit (TIGRA) et les Honeypot (HP/HN).

Cette étude avait pour objectif d'étudier les techniques et expérimentations actuelles consacrées à la dissimulation et la fuite d'information au sens large, et orientée particulièrement sur les problèmes de sécurité suscités pour les réseaux sensibles ; elle avait pour ambition de permettre l'identification de ce type de vulnérabilités, et dans la mesure du possible d'y associer des contre-mesures.

Cette étude partait du principe que les failles de sécurité, dans le cadre d'un échange d'information, ne se situent plus à partir de la couche réseau[8] (niveau 2 du modèle OSI) mais à partir de la couche application (niveau 7 du modèle OSI) ; elle s'est déroulée en parallèle de l'étude destinée à sécuriser le transfert de données entre deux réseaux de sensibilités différentes (Cf. Passerelle inter-réseaux) [9].

Dans le cadre de ces échanges d'information, EFFICACE nous a amenés à distinguer deux notions :

- l*a dissimulation* qui désigne le fait de rendre invisible une donnée. Typiquement, il peut s'agir d'une donnée cachée au sein d'une autre, au sein d'un système de fichier, d'un processus tournant en tâche de fond et non visible pour un utilisateur ;
- l*a fuite* qui fait référence à un transfert d'information non désiré notamment par l'usage de canaux cachés. Une illustration de ce concept est la récupération d'informations sensibles présentes au sein d'un réseau local sécurisé depuis un poste situé sur l'Internet par l'utilisation de failles protocolaire.

Cette étude est partie des considérations suivantes :

- toute information est susceptible de contenir de l'information cachée
- la vérification de la présence d'une donnée dissimulée n'est pas l'objet de cette étude (même si cela a été réalisé à titre indicatif)
- un opérateur peut à tout moment vérifier les données échangées sur un réseau.

Outre ces principes, des limites ont été inclues à notre étude car chaque technique évoquée au sein de ce document pourrait faire l'objet d'une étude à par entière :

- cet état de l'art porte uniquement sur les réseaux de type IPv4 et failles liées aux protocoles TCP/IP,

[8] Il existe déjà , en effet, un certains nombre de solutions, dont l'équipement FOX de THALES, qui permettent de réduire considérablement les risques de vulnérabilités liées aux couches réseaux.

[9] L'objectif de SESAME est de se prémunir contre tout transfert d'information violant la politique de sécurité en vigueur pour les réseaux sensibles.

- l'aspect mathématique n'a pas été abordé.

6.2 Quelques Eléments constitutifs de l'étude

6.2.1 Les techniques employées dans le processus de transfert et de fuite de l'information

Les faiblesses des éléments constitutifs d'un réseau

- **Les IDS** détection des vulnérabilités connues uniquement et aucune protection sur les transactions sécurisées SSL
- **Les pare-feux** agissent généralement exclusivement sur le type des communications mais pas sur leur contenu

Les faiblesses protocolaire

- **Exploitation de l'en-tête TCP/IP** construction de faux paquets en utilisant certains champs des en-têtes IP et TCP
- **Exploitation de champs d'en-tête inexploités** Ex : TCP et IGMP
- **Exploitation de la zone de bourrage**
- **L'encapsulation protocolaire** ex :encapsuler des requêtes dans des paquets ICMP dont les champs optionnel sont enregistrés et non vérifié (route empruntée par la trame, temps de parcours)

Le tunneling permet d'utiliser des protocoles non autorisés à travers un pare-feu

Les troyens remplissent des fonctions non désirées, inconnues de l'utilisateur

Les spywares programmes conçu dans le but de collecter des données personnelles sur ses utilisateurs. Ces données sont généralement envoyées à son concepteur

6.2.2 La stéganographie

Quelques exemples de techniques de stéganographie étudiées.

Substitution d'information et espaces réservés

- **Substitution des bits de poids faible** remplacement des bits de poids faible de codage d'un pixel d'une image (JPEG, GIF) par d'autres bits d'information
- **Permutations pseudo-aléatoires** incorporation d'informations dans les propriétés statistiques de la luminance des pixels (ex : *Outguess*)
- **Les bits de redondance** écrasement de bits redondants par d'autres bits d'information
- **Réorganisation de la palette de couleurs** réorganisation obtenue par la modification des bits de poids faibles du codage des pixels
- **Dissimulation dans des fichiers binaires**
- **Exploitation d'espaces inutilisés au sein d'un ordinateur**
- **Les système de fichiers stéganographique** (les systèmes de fichiers stéganographiques eux-mêmes qui offrent deux niveaux logiques de stockage d'information, et les espaces interstitiels, utilisation de l'espace de stockage alloué à un fichier et non utilisé)

- **Exploitation du système de fichiers NTFS** exploitation des flux de fichiers, ou ADS

Les techniques de transformée

- **Transformation en Cosinus Discret** cette méthode exploite le fait que les valeurs calculées par l'utilisation de cette transformée ne sont pas précises, ainsi la répétition de tels calculs conduit à une limitation de la précision et à l'introduction d'erreurs
- **Stéganographie appliquée à un fichier audio** la dissimulation d'information dans les plages de fréquences inaudible à l'oreille humaine

L'approche statistique méthode utilisée afin de leurrer les outils de stéganalyse

Encodage d'information dans un texte texte dans le texte, mots codes ou synonymes, ajout d'espaces à la fin des phrases ou espacement entre les mots

Techniques appliquées aux documents propriétaires

- **Adobe** utilisation de l'option du menu Document/Recadrer pour cacher les marges
- **MS-Office** informations « propriété », inclusion automatique de données (INCLUDTEXT), utilisation éditeur hexadecimal (*UltraEdi*t)

MS OUTLOOK et MS EXCHANGE exploitation du fichier winmail.dat

6.2.3 Le Watermarking : état de l'art

Le watermarking diffère de la stéganographie par le fait que l'on se limite souvent à dissimuler très peu d'information (très souvent un seul bit) dans l'image hôte et a pour objectif de démontrer l'intégrité du document ou encore d'en protéger les droits d'auteur.

Les techniques de marquage

- **Modification des bits de poids faible** les premiers algorithmes allaient inscrire la marque dans les bits de poids faible de la luminance de l'image
- **Technique du "Patchwork"** répétition un grand nombre de fois du même bit pour qu'une étude statistique donne le bit marqué
- **Algorithme de Koch et Zhao** marquage d'un bit sur les moyennes fréquences correspondant à un calcul de transformée en cosinus discrète
- **Watermarking par étalement de spectre** envoi d'un message sur un grand spectre de fréquences de telle manière que, à toute fréquence, la puissance du signal émis soit inférieure au bruit

Les traitements malveillants

- **L'attaque par mosaïque** effacement de signature par morcellement d'image
- **Stirmark** banc de test permettant d'apprécier la robustesse d'un schéma de tatouage d'image appliquant principalement des distorsions géometriques

6.3 Environnement Technique étudié

6.3.1 Quelques outils stéganographiques

Médium de type texte

- **TextHide** *Syst. Unix, Windows* dissimule des données par l'intermédiaire d'un dictionnaire de synonymes
- **StegParty** *Syst. Unix* utilise la ponctuation
- **Snow** *Syst. Unix* utilise les tabulations et les espaces de fin de ligne
- **NiceText** *Syst. Unix* utilise un dictionnaire de synonymes
- **FFEncode** *Syst. DOS* dissimulation d'information par l'intermédiaire de caractères nuls utilisant un code de type morse

Médium de type image

- **Invisible Secrets** *Syst. Unix, Windows* dissimulation d'un message dans de nombreux types de fichier (JPEG, PNG, BMP, HTML et WAV).
- **Gifshuffle** *Syst. Unix, Windows* permutation des couleurs dans la palette
- **JPegX** *Windows* que JPG
- **BMP Secrets** *Windows* que BMP
- **Digital Picture Envelope** *Windows*
- **CryptArkan** *Windows* dissimule des données dans une image BMP ou un fichier audio de type WAV
- **Cameleon** *Windows* chiffrement AES 256 bits pour des données cachées
- **JSteg Shell** *Syst. Unix, Windows*
- **Outguess** *Windows* seul programme qui reste indétectable par ***Stegdetect 0.2***

Médium de type fichier audio

- **WeavWav** *Freeware, Windows* dissimulation d'information dans un fichier de type WAV
- **Stego-Lame** *Freeware, Windows* différents formats (MP3, Ogg Vorbis, etc.)
- **MP3Stego** *Freeware, Windows, Syst. Unix* peut également servir comme outil de marquage de fichier MP3

Médium de type fichier compressé

- **GZSteg** *Freeware, DOS* dissimule de l'information au sein d'un fichier de type GZip

Médium de type document propriétaire

- **FactMiner** permet d'extraire un grand nombre d'informations sur l'auteur du document, le produit d'édition utilisé, la langue, etc. Ce logiciel est appliquable aux documents de types texte, RTF, HTML, SGML, XML, PDF, PostScript

6.3.2 Quelques Exemple de troyens

ACK Cmd permet d'établir une communication entre un attaquant et un serveur par l'envoie de segments ACK ("Ack Tunneling").

Gatslag combinaison entre un tunnel et un troyen, il exploite les faiblesses d'Internet Explorer

SETIRI version améliorée du troyen ***Gatslag*** il ne contient aucune commande exécutable susceptible d'être bloquée par un pare-feu

Chapitre 7 - Conclusion

Tous ces aspects restent à conforter par les réalisations et études internes relatives aux :

- Systèmes et équipements utilisables dans un cadre OTAN (ex : chiffrement IP agréé OTAN TCE621, chiffreur Echinops (agrément OTAN en cours), système de contrôle d'accès au postes Minicita)
- Equipements et architectures techniques de protection de bordure des système opérationnels de coalition (sécurisation des WAN de théâtre, interconnexion de systèmes multi-niveaux de sécurité, passerelles, etc.)
- Outils et études dans le cadre de la maîtrise de l'information et de la gestion de l'environnement psychologique (PSYOPS)
- Etudes VAR

Références

[1] projet **TIRI** (Tests d'Intrusions dans les Réseaux Informatiques), réalisé par *Sébastien Breton* premier semestre 2000

[2] projet **CCSI** (Configuration Centralisée des Systèmes d'Information) réalisé par *Vincent Bechet* septembre 2001

[3] projet **HP&HN** (HoneyPot & Honeynet) réalisé par *Franck Crepel* premier semestre 2002

[4] projet **TIGRA** (Tests d'Intrusion et Génération de Rapports d'Audit) réalisé par *Patricia Cabanel* premier semestre 2002

[5] projet **SESAME** (Système d'EchangeSécurisé pour un Accès Multi-niveau Expérimental) réalisé par *Renaud SCHAUBER* et *Arnaud KEMP* octobre 2003

[6] projet **EFFICACE** (Elaboration Furtive de Fuite d'Information CAChés atemporels d'Evasion) réalisé par *Sébastien POLLET* Septembre 2003

[7] Projet **THONIC** (synthèse des autres travaux) réalisée par *Vincent Ribaillier* octobre 2002

Intrusion – Réaction – Appât

Symposium NATO/RTO/IST
Vacher Emmanuel
Toulouse – 19 et 20 avril 2004

THALES

Sommaire

Introduction

- Le concept de « défense en profondeur » préconise la succession de barrières de protection concentriques et indépendantes autour du SI
- Première défense vis à vis de l ’extérieur, la protection de bordure (Boundary Protection Services pour l ’OTAN) cumule de nombreuses technologies (IPS, Firewall, antivirus, technologies de DMZ, …)
- Les éléments présentés ci-après et ayant fait l ’objet d ’études THALES, concernent ce type de BPS :
  - Techniques d ’Intrusion dans les Systèmes d’Information
  - Fuite d’informations (Canaux Cachés)
  - Systèmes de détection d’intrusion
  - Appâts (Honeypots / Honeynets)
  - Passerelle de protection

Intrusion – Réaction – Appât

Attaques et Intrusions

THALES

Contexte Etude sur Intrusions

- Les études ont porté sur les outils et les méthodes d'intrusion
  - Analyse des méthodes d'attaque des systèmes d'information
  - Analyse des outils disponibles
  - Analyse des vulnérabilités exploitées

… et ont montré la nécessaire adaptation des méthodes de protection

  - Une défense plus dynamique (évolution vers les Systèmes de Protection contre les Intrusions IPS)
  - Complétant une défense passive (Honey Pot & Honey Net)
  - Et un traitement des fichiers d 'audit couvrant de longues périodes

… dans le cadre d 'une politique de sécurité cohérente

  - **moindre privilège** (contrôle d 'accès et besoin d 'en connaître)
  - **Minimalité**. Seuls les protocoles et services inter-réseaux et les instructions correspondantes nécessaires à l'exécution de la mission opérationnelle seront autorisés par l'interconnexion
  - **Noeud autoprotégé (SPN)**. Chaque SIC interconnecté traitera initialement les autres SIC comme non fiables et appliquera des mesures de protection pour contrôler l'échange d'information avec les autres systèmes

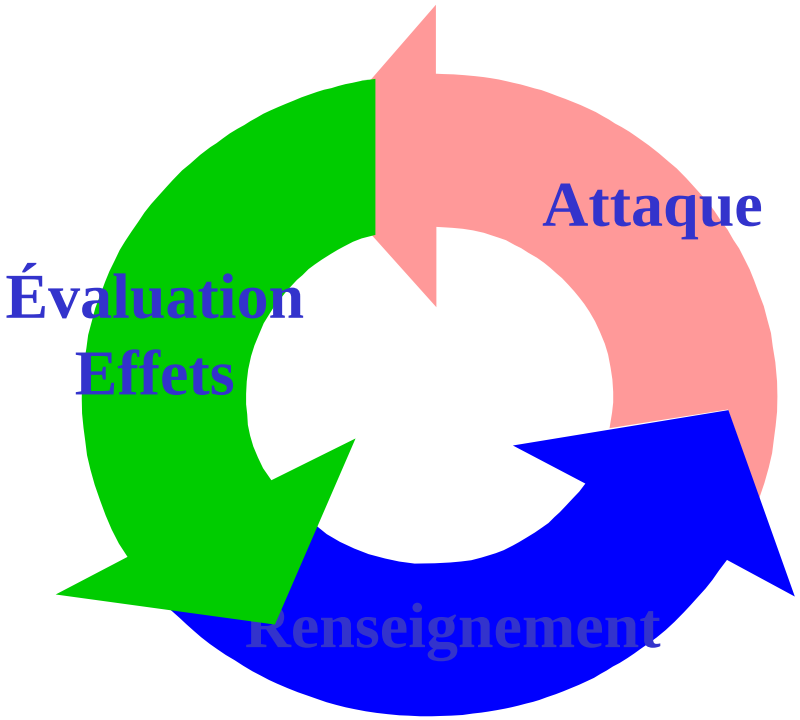
Principales Techniques d'attaque étudiées

- Les Techniques d'intrusion étudiées ont été regroupées selon deux catégories
  - **Attaques physiques**
    - Interception, balayage, écoute, piégeage, …
  - **Attaques logiques**
    - Fouille, Craquage de mots de passe, Déguisement, Mystification, Rejeu, Substitution, Déni de service, Cheval de Troie, Trappe et faille, Bombe, Virus, Vers, Cryptanalyse, …

- Les principaux outils utilisés provenaient du Web
  - Bombes e-mail (Kaboom, Anonymail, Homicide, Avalanche, …)
  - Craquage de mot de passe (NTUCrack, John The Ripper, L0phtCrack, …)
  - Déni de service (Winnuke, Killwin, Bitchslap, …)
  - Sniffeurs (Ethereal, Analyser, …)
  - Scanners (Ultrascan, nmap, …)
  - Chevaux de Troie (Netbus, BackOrifice, …)

Méthodes d ’Attaque

Cycle d ’une attaque



Scénario classique d ’attaque

Renseignement
Écoute, Recherches, Espionnage

Préparation (mise en mode dégradé)
Saturation, brouillage, désinformation

Intrusion
Usurpation, Cheval de Troie, Exploitation failles

Installation
Porte dérobée, Canaux cachés

Camouflage
Effacement trace, Inhibition surveillance

Propagation
Rebond, Virus, Vers

Attaque
Destruction, Altération, Espionnage

Etude sur la Détection d'Intrusion

Les études ont porté sur l 'état de l 'art et la mise en œuvre des outils de détection d 'intrusion IDS

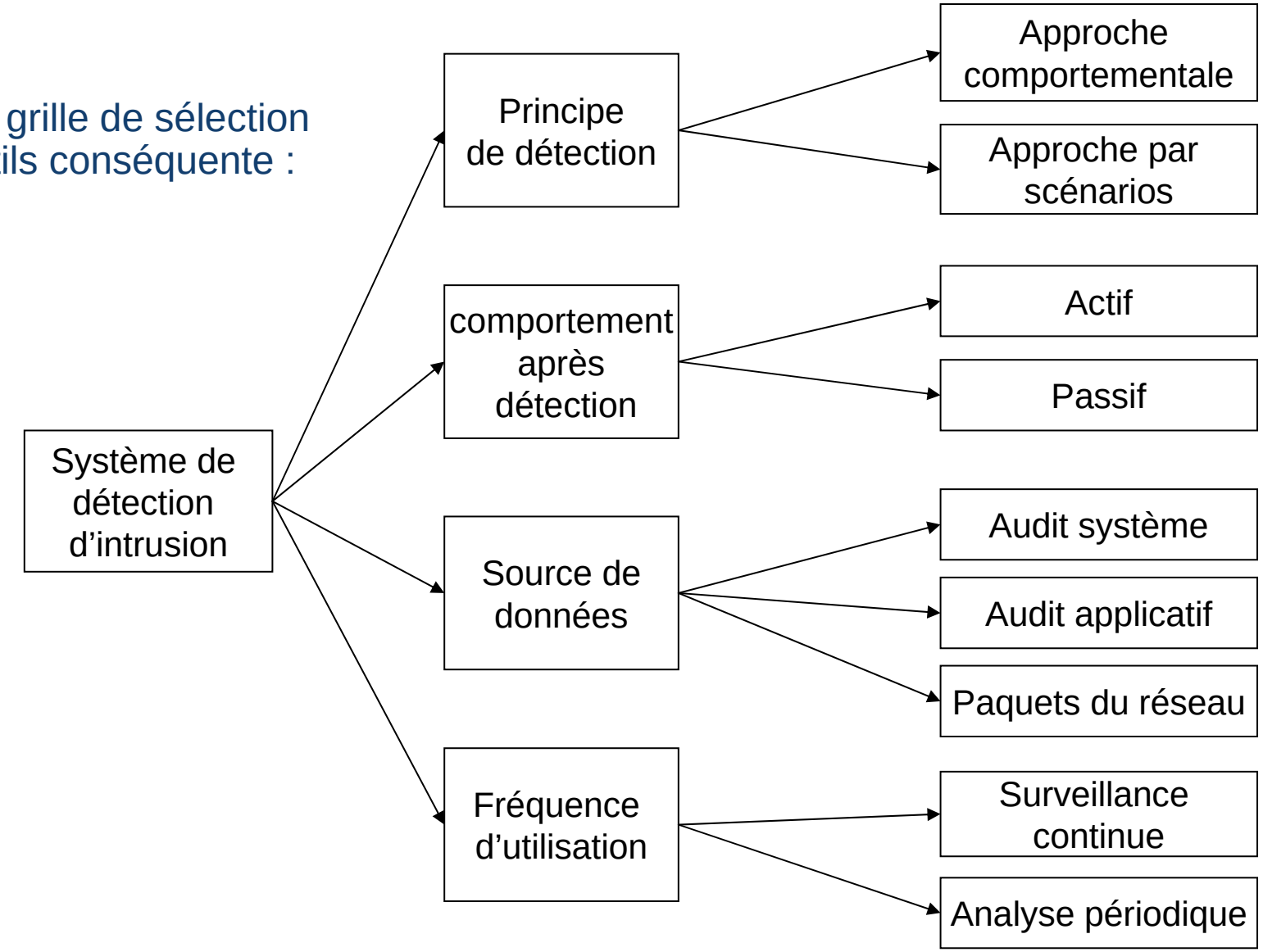
- Elles ont montré une grande diversité de fonctionnalités pouvant couvrir :
  - Détection (signature ou analyse comportementale)
  - réaction (alarme, coupure, reconfiguration firewall, dérivation)
  - analyse sur données d 'audit ou flux
- Une intégration possible en plusieurs endroit du SI
  - en bordure de réseaux pour analyser les flux en entrée / sortie « Network Based IDS »
  - sur les réseaux « Host Based IDS »
- Une fragilité liée à :
  - difficile équilibre entre faux-négatifs et faux-positifs
  - deviennent la cible de certaines attaques par saturation

Systèmes de détection d'intrusion

- Définition
  - Principe de fonctionnement des IDS
    - Détection des attaques
    - Réaction aux attaques
    - Avertissement local et/ou vers le responsable SSI
    - Analyse
  - Mode d'action des IDS
    - Mode furtif
    - Mode coupure
    - Mode écoute
  - Paramètres de classification des IDS
    - Principe de détection (comportementale, scénario)
    - Comportement après détection (Actif / Passif)
    - Sources de données (audit système / audit applicatif / paquets réseau)
    - Fréquence d'utilisation (temps réel / analyse périodique)

Systèmes de détection d'intrusion (types)

D 'où la grille de sélection des outils conséquente :



Systèmes de détection d'intrusion (outils)

- Les principaux outils utilisés provenaient du Web
  - N-IDS (Network Based IDS) *Snort, BlackIce, Cisco Secure IDS ou NetRanger, Shadow, RealSecure*
  - H-IDS (Host Based IDS): *Swatch, RealSecure OS Sensor, Intruder Alert*
  - File Integrity Checkers: *Tripwire, AIDE, Intact* ou *Integrit*
  - autres types d'IDS :
    - Honeypots (logiciel *Deception Toolkit*) et les Honeynets
    - Hybrid IDS (*CyberCop Monitor ou CentraxICE*) regroupent les fonctionnalités d'un N-IDS et d'un H-IDS
    - Network Node IDS (NN-IDS) supervision d'un groupe de machines
    - C-IDS (pour *Comportemental IDS*)

Cas particulier des Canaux Cachés

Les études ont porté essentiellement sur l'état de l 'art et ont mis en évidence deux notions « complémentaires »

- la *dissimulation* qui désigne le fait de rendre invisible une donnée
- la *fuite* qui fait référence à un transfert d'information non désiré

- Elles ont montré que ces canaux cachés utilisaient certaines faiblesses
  - **de certains éléments de protection**
    - IDS (aucune action sur flux sécurisés comme SSL)
    - Firewall (peu ou pas d 'action sur le contenu)
  - **des protocoles**
    - Exploitation de champs d'en-tête inexploités ou non contrôlés (TCP/IP)
    - Exploitation de la zone de bourrage
    - L'encapsulation protocolaire
  - **Le tunneling**
  - **Les troyens et spywares**

Cas particulier des Canaux Cachés

- Les principales techniques étudiées
  - **stéganographie**
    - Substitution d'information et espaces réservés
      - Substitution des bits de poids faible
      - Permutations pseudo-aléatoires
      - bits de redondance
      - Dissimulation dans des fichiers binaires
      - Exploitation du système de fichiers NTFS
    - Les techniques de transformée
      - Transformation en Cosinus Discret
      - appliquée à un fichier audio
    - L'approche statistique
    - Encodage d'information dans un texte
  - **Watermarking**
    - Modification des bits de poids faible
    - Technique du "Patchwork"
    - Watermarking par étalement de spectre

Cas particulier des Canaux Cachés

- Les principaux outils étudiés
  - **stéganographiques**
    - **Texte** (TextHide , StegParty , Snow , FFEncode , …)
    - **image** (Invisible Secrets , Gifshuffle , CryptArkan , Cameleon , Outguess , …)
    - **audio** (WeavWav , Stego-Lame , MP3Stego)
    - **fichier** compressé (GZSteg)
  - **troyens**
    - ***ACK Cmd*** permet d'établir une communication entre un attaquant et un serveur par l'envoie de segments ACK ("Ack Tunneling").
    - ***Gatslag*** combinaison entre un tunnel et un troyen
    - ***SETIRI*** version améliorée du troyen *Gatslag*

Intrusion – Réaction – Appât

Honeypots & Honeynets

THALES

Honeypots & Honeynets

Un concept simple à l ’application parfois complexe, l’étude à mis en évidence les aspects suivants :

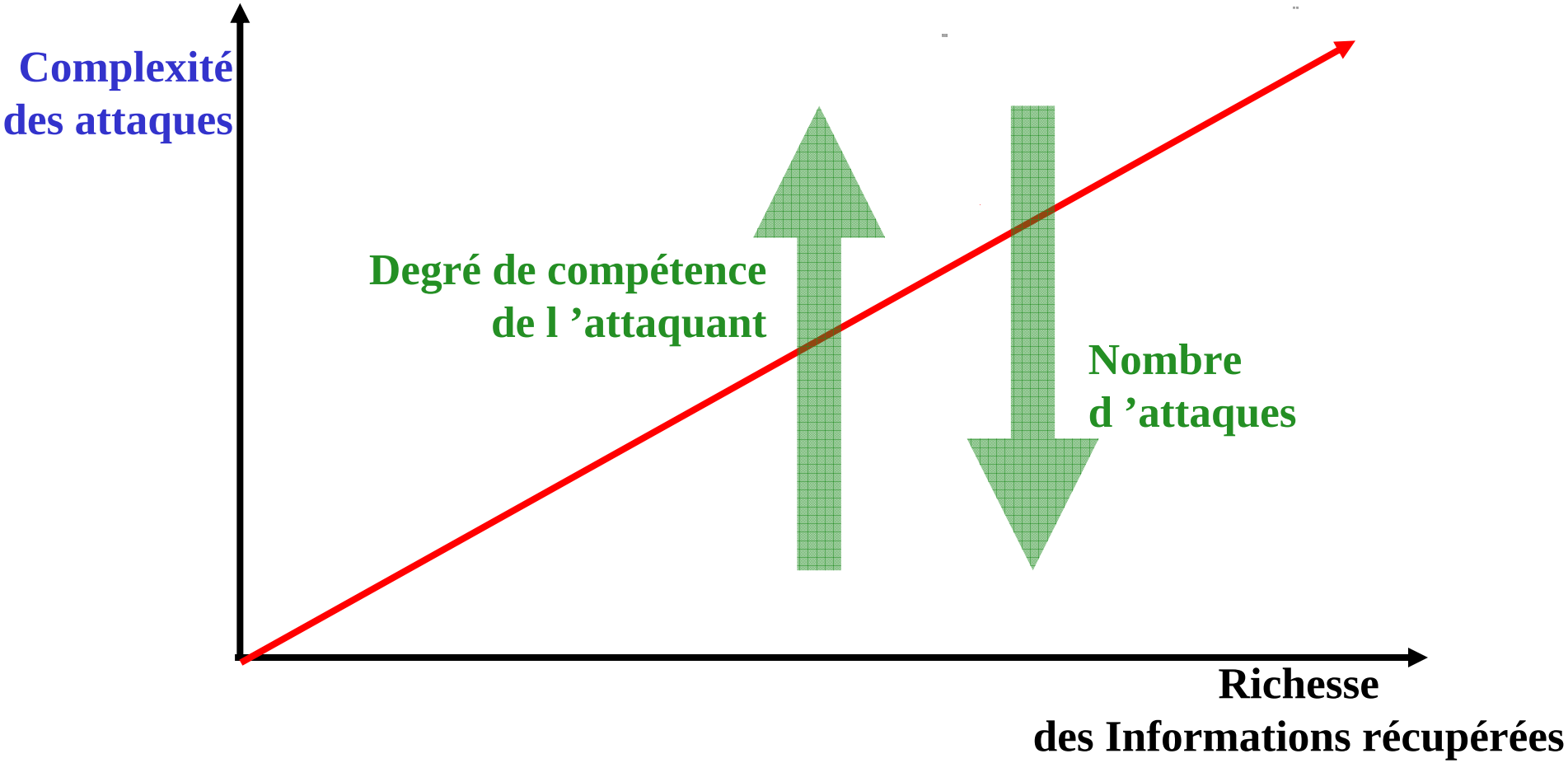
- La notion de « Pot de miel » peut s ’étendre d ’un simple leurre (mot de passe constructeur conservé) à des environnement dédié (réseaux complets)
- Les objectifs d ’un HP/HN peuvent aller de la simple détection d ’une attaque, à l ’étude des attaques et attaquants (voire la désinformation)
- Ces systèmes doivent être réfléchis du fait de la notion de piège (aspects juridiques) et des risques d ’utilisation pour rebond (environnement volontairement sous-protégé)

les apports principaux sont :

- complément aux systèmes de protection contre les intrusions
- identification des attaques et pirates
- connaissance des nouvelles attaques et scénarios

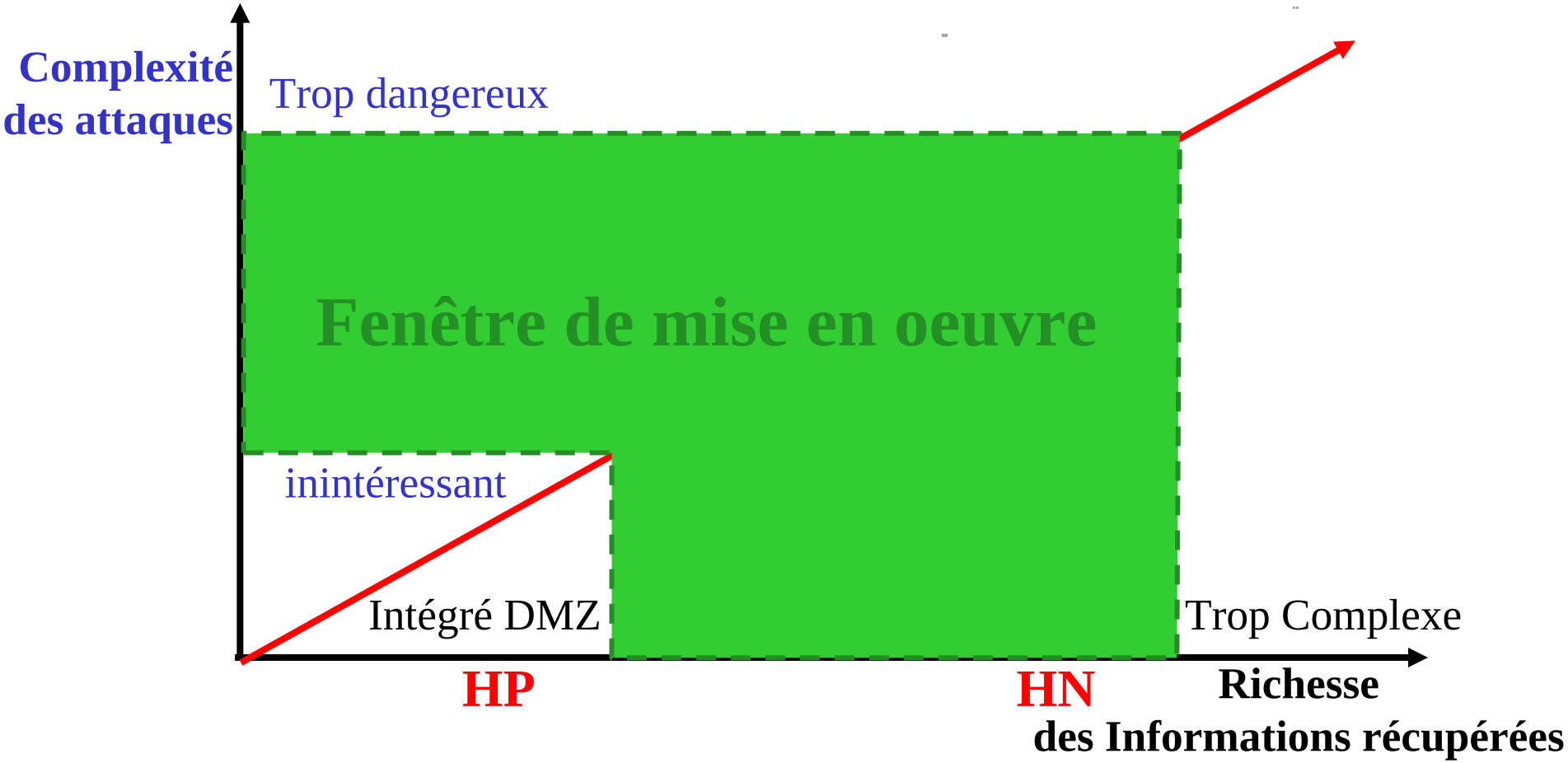
Honeypots & Honeynets (choix)

HP / HN : typage des attaques



Honeypots & Honeynets (paramétrage)

HP / HN : fenêtre de mise en œuvre



Intrusion – Réaction – Appât

Passerelles inter-domaines

Passerelles inter-domaines

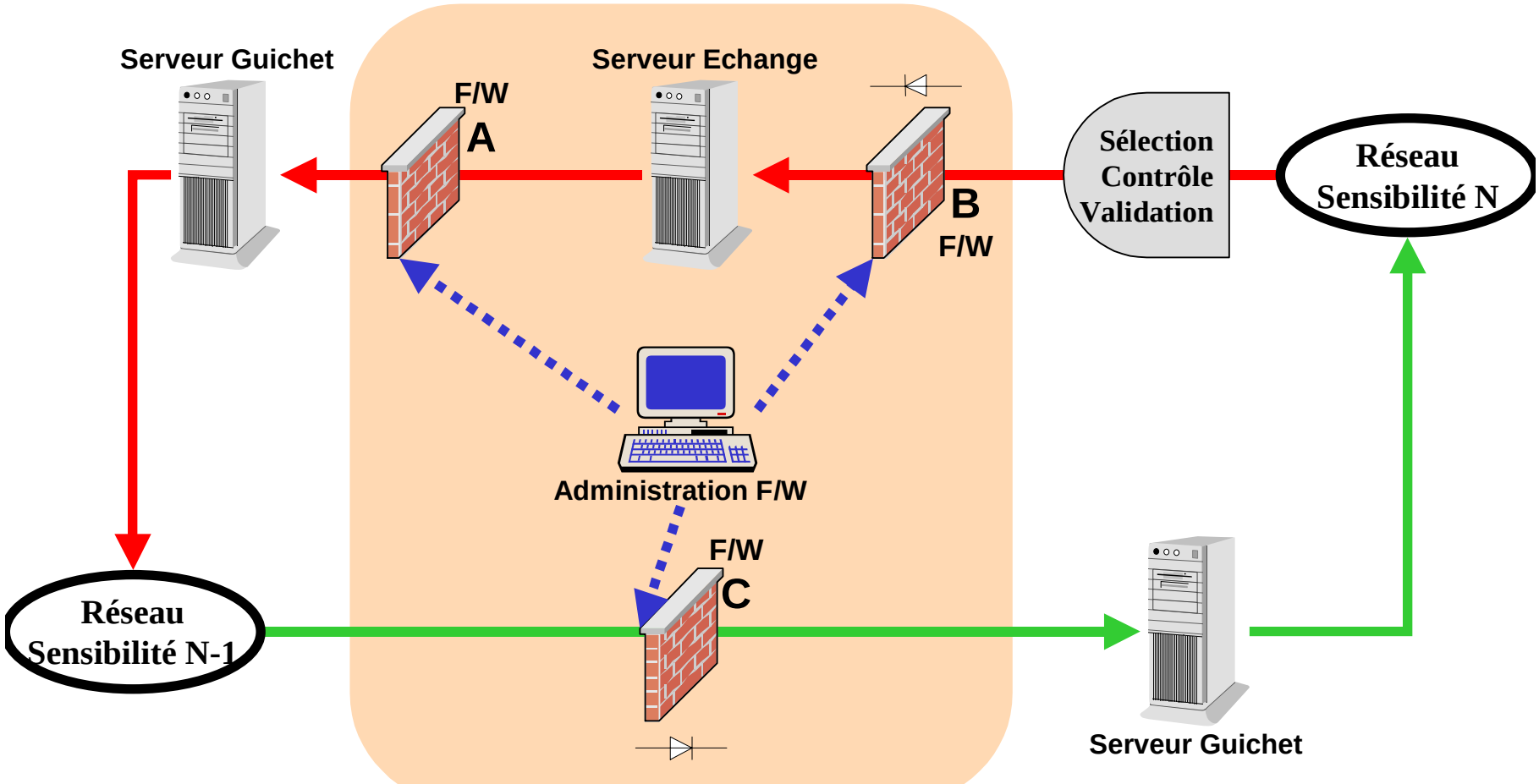
- Les SI nécessitent de plus en plus d'échanges d'information y compris entre domaines de sensibilité (classification) différente
- la diversité des attaques sur les media de communication ainsi que le nécessaire cloisonnement (réglementation) entre domaines de sensibilité différente implique la réalisation de passerelles sécurisée
- Les objectifs de cette passerelle inter-domaines :
  - échanges limités et contrôlés entre 2 domaines de sensibilité différente
  - protection de bordure (intrusions, antivirus)
  - Contrôle des canaux cachés
  - Contrôle des informations échangées entre les deux réseaux interconnectés (sensibilité, type
  - Contrôle des droits et signatures (autorisations)

Passerelles inter-domaines

- Composition de cette passerelle inter-domaines :
  - Un « SAS automatisé » ou serveur d ’échange : cœur de cette passerelle, il doit être indépendant des deux réseaux interconnectés
  - Un système de marquage certifié (labellisation) permettant de reconnaître la qualité de l ’information qui transite sur le SAS
  - Un système de validation sur le domaine le plus sensible permettant de contrôler les informations « descendantes »
  - Un système de PKI permettant les contrôles sur les échanges (marquage, signature, droits)
  - Un ensemble de firewall permettant la mise en œuvre des protections en bordure

Passerelles inter-domaines

Passerelle de type hybride



Conclusion

- Premier maillon d ’une défense en profondeur, un système de protection de bordure (Boundary Protection Services) devrait regrouper tous ces composants en un tout cohérent

- Leur intégration ne doit pas simplement être abordée du point de vue technique, mais correspondre à une véritable politique de sécurité à l ’interconnexion (protocole) qui doit prendre en compte les spécificité des domaines ou réseaux interconnectés (politiques de sécurité) ainsi que leurs missions

Merci de votre attention